APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/885,750	06/19/2001	Scott A. Hankins	011.0215.01	4021

22895   7590   08/03/2004

PATRICK J S INOUYE P S
810 3RD AVENUE
SUITE 258
SEATTLE, WA 98104

EXAMINER
KLINGER, SCOTT M

ART UNIT	PAPER NUMBER
2153	

DATE MAILED: 08/03/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 June 2001*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is

closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-38* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18 and 20-37* is/are rejected.

7)☒ Claim(s) *19, 38* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage

        application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____ .

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____ .

DETAILED ACTION

Claims 1-38 are pending.

Priority

No claim for priority has been made. The effective filing date for subject matter in the application is 19 June 2001.

Claim Objections

Claims 19 and 38 are objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent claim should refer to other claims in the alternative only. See MPEP § 608.01(n). Accordingly, the claims have not been further treated on the merits.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-4, 8-11, 17, 18, 20, 23, 25, 26, 28, 32, 34, 35, and 37 are rejected under 35 U.S.C. 102(e) as being anticipated by Rakoshitz et al. (U.S. Patent Number 6,578,077, hereinafter "Rakoshitz"). Rakoshitz discloses a traffic monitoring tool for bandwidth management. Rakoshitz shows,

In referring to claim 1,

- A flow analyzer analyzing flow characteristics of network traffic comprising a multiplicity of transient packets each including a parameterized header, comprising a parser retrieving operational characteristics from the parameterized header of each such transient packet generated by a plurality of intercommunicating applications; a comparator identifying a proscribed application by comparing the operational characteristics to stored characteristics unique to the proscribed application; and

  "Flow Analysis and Session Tagging ("FAST") implements rich, application level traffic classification, and measurement. This operation is accomplished without introducing slow data paths to minimize latency and maximize overall throughout of traffic through the tool management engine. As shown in the Fig., the FAST module provides for classification 203 of information such as parameters 213 including application, presentation, session, transport, and network. The FAST module also provides for measurement 219 of various parameters. The FAST module is coupled to the API." (Rakoshitz, col. 12, lines 23-33)

  "categorizing the data rate from the flow of information based upon at least one of a plurality of traffic classes" (Rakoshitz, col. 3, lines 7-9)

- A flow monitor controlling transmission of each such transient packet subsequently exchanged with the proscribed application:

  "Flow Analysis and Intelligent Regulation ("FAIR") implements traffic control based on a combination of flow control and queuing algorithms. FAIR's objective provides inbound and outbound traffic management for meaningful time intervals, reducing the load on packet classifiers and packet schedulers. The FAIR module controls 205 incoming and outgoing information to and from the network. Additionally, the FAIR module controls 205 by parameters 215 such as class, session, burst, packet, and others." (Rakoshitz, col. 12, lines 38-47)

In referring to claim 2,

- A classifier classifying a connection to the proscribed application by examining connection initialization operational characteristics:

  Rakoshitz, col. 12, lines 23-33 (see full quote above)

  A system that provides for the classification of session parameters inherently implies examining connection initialization operational characteristics

In referring to claim 3,

- A classifier classifying a login to the proscribed application by examining session initiation operational characteristics:

  Rakoshitz, col. 12, lines 23-33 (see full quote above)

  A system that provides for the classification of session parameters inherently implies examining session initiation operational characteristics

In referring to claim 4,

- A classifier classifying a raw data flow to the proscribed application by examining data flow operational characteristics:

  Rakoshitz, col. 12, lines 23-33 (see full quote above)

  A system that provides for the classification of session and transport parameters inherently implies examining data flow operational characteristics

In referring to claim 8,

- The operational characteristics comprise at least one of a network address, port and traffic direction flow:

  Rakoshitz, col. 12, lines 23-33 (see full quote above)

  A system that provides for the classification of application, presentation, session, transport, and network parameters inherently implies examining network addresses, ports and traffic direction flow

In referring to claim 9,

- The transient packets are communicated via the TCP/IP protocol:

  "the present invention can be applied to manage a variety of TCP/IP network traffic types for the Internet and Intranet." (Rakoshitz, col. 21, lines 45-47)

In referring to claim 10,

- Analyzing flow characteristics of network traffic comprising a multiplicity of transient packets each including a parameterized header:

  "the present invention provides a novel computer network system having a real-time bandwidth-profiling tool" (Rakoshitz, col. 2, lines 56-58)

- Retrieving operational characteristics from the parameterized header of each such transient packet generated by a plurality of intercommunicating applications:

  Rakoshitz, col. 12, lines 23-33 (see full quote above)

- Identifying a proscribed application by comparing the operational characteristics to stored characteristics unique to the proscribed application:

  Rakoshitz, col. 3, lines 7-9 (see full quote above)

- Controlling transmission of each such transient packet subsequently exchanged with the proscribed application:

  Rakoshitz, col. 12, lines 38-47 (see full quote above)

In referring to claim 11,

- Classifying a connection to the proscribed application by examining connection initialization operational characteristics:

  Rakoshitz, col. 12, lines 23-33 (see full quote above)

  A system that provides for the classification of session parameters inherently implies examining connection initialization operational characteristics

In referring to claim 12,

- Classifying a login to the proscribed application by examining session initiation operational characteristics:

  Rakoshitz, col. 12, lines 23-33 (see full quote above)

  A system that provides for the classification of session parameters inherently implies examining session initiation operational characteristics

In referring to claim 13,

- Classifying a raw data flow to the proscribed application by examining data flow operational characteristics:

  Rakoshitz, col. 12, lines 23-33 (see full quote above)

  A system that provides for the classification of session and transport parameters inherently implies examining data flow operational characteristics

In referring to claim 17,

- Characteristics comprise at least one of a network address, port and traffic direction flow:

  Rakoshitz, col. 12, lines 23-33 (see full quote above)

  A system that provides for the classification of application, presentation, session, transport, and network parameters inherently implies examining network addresses, ports and traffic direction flow

In referring to claim 18,

- The transient packets are communicated via the TCP/P protocol.

  Rakoshitz, col. 21, lines 45-47 (see full quote above)

In referring to claims 20 and 29,

- A flow monitor monitoring a network connection supporting a flow of network traffic in a distributed computing environment:

  Rakoshitz, col. 12, lines 23-33 (see full quote above)

- The network traffic flow comprising a stream of data packets generated by a rogue application and incrementally adjusting bandwidth allocated to the monitored network connection until the flow of the network traffic for the rogue application achieves a steady state of bandwidth restriction; a traffic manager controlling the flow of subsequent network traffic over the monitored network connection at the steady state of bandwidth restriction:

  "adjusting said bandwidth allocation so that said allocation depends upon a type of said flow" (Rakoshitz, claim 57)

  Rakoshitz, col. 12, lines 38-47 (see full quote above)

  A system that allocates specific bandwidth to specific applications inherently implies controlling the flow of traffic at a steady state of bandwidth restriction

In referring to claim 23,

- The flow monitor storing the steady state of bandwidth restriction as a retrievable traffic flow control:

  "The traffic management cycle is depicted as a continuous cycle, which includes a monitoring phase 301, a creating/applying policy phase 303, and a reporting/alarming phase 305, but is not limited to these cycles." (Rakoshitz, col. 10, lines 3-7)

  A system that allocates bandwidth based on stored policies inherently implies storing the steady state of bandwidth restriction as a retrievable traffic flow control

In referring to claim 25,

- A flow analyzer examining at least one of a network address, port and characteristics stored as parameters in a header of each such packet:

  Rakoshitz, col. 12, lines 23-33 (see full quote above)

A system that provides for the classification of application, presentation, session, transport, and network parameters inherently implies examining network addresses, ports and traffic direction flow

In referring to claim 26,

- The flow monitor monitoring a redirected packet flow facilitated by the rogue application:

  Rakoshitz, col. 2, lines 56-58 (see full quote above)

  The flow monitor monitors all of the packets.

In referring to claim 28,

- The rogue application executes in compliance with the TCP/IP protocol:

  Rakoshitz, col. 21, lines 45-47 (see full quote above)

In referring to claim 32,

- Storing the steady state of bandwidth restriction as a retrievable traffic flow control.

  Rakoshitz, col. 10, lines 3-7 (see full quote above)

  A system that allocates bandwidth based on stored policies inherently implies storing the steady state of bandwidth restriction as a retrievable traffic flow control

In referring to claim 34,

- Examining at least one of a network address, port and characteristics stored as parameters in a header of each such packet:

  Rakoshitz, col. 12, lines 23-33 (see full quote above)

  A system that provides for the classification of application, presentation, session, transport, and network parameters inherently implies examining network addresses, ports and traffic direction flow

In referring to claim 35,

- Monitoring a redirected packet flow facilitated by the rogue application:

  Rakoshitz, col. 2, lines 56-58 (see full quote above)

  The flow monitor monitors all of the packets.

In referring to claim 37,

- The rogue application executes in compliance with the TCP/IP protocol:

  Rakoshitz, col. 21, lines 45-47 (see full quote above)

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 5-7, 14-16, 21, 22, 24, 27, 30, 31, 33, and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rakoshitz.

In referring to claim 5, although Rakoshitz shows substantial features of the claimed invention, including the system of claim 1 (see 102 rejection above), Rakoshitz does not show a traffic manager incrementally restricting bandwidth allocated to the network traffic specifically exchanged with the proscribed application until an evasive action is detected. Nonetheless this feature is well known in the art and would have been an obvious implementation of the system disclosed by Rakoshitz.

Rakoshitz discloses that certain applications are bandwidth-sensitive: *"In a specific embodiment, synchronous, interactive, and real-time applications, which are bandwidth-sensitive, can require minimum bandwidth guarantees, and can require sustained and burst-*

scale bit-rates" (Rakoshitz, col. 4, lines 58-62). Rakoshitz also discloses the traffic management cycle continuously creates/applies policies as well as reports/alarms: *"The traffic management cycle is depicted as a continuous cycle, which includes a monitoring phase 301, a creating/applying policy phase 303, and a reporting/alarming phase 305, but is not limited to these cycles."* (Rakoshitz, col. 10, lines 3-7)

Given these teachings, a person of ordinary skill in the art would have readily recognized the desirability and advantages of implementing the system of Rakoshitz so as to incrementally restrict bandwidth allocated to the network traffic specifically exchanged with the proscribed application until an evasive action is detected, in order to determine a minimum bandwidth requirement, as discussed in Rakoshitz.

In referring to claim 6, in the implementation of the system of Rakoshitz discussed above, it would be obvious to record the minimum bandwidth level determined by decreasing the bandwidth, so as to provide the bandwidth required by the rogue application.

In referring to claim 7, in the implementation of the system of Rakoshitz discussed above it would be obvious to increase the bandwidth to the minimum level determined by decreasing the bandwidth below the threshold, so as to provide the bandwidth required by the rogue application.

In referring to claim 14, although Rakoshitz shows substantial features of the claimed invention, including the system of claim 10 (see 102 rejection above), Rakoshitz does not show incrementally restricting bandwidth allocated to the network traffic specifically exchanged with the proscribed application until an evasive action is detected. Nonetheless this feature is well known in the art and would have been an obvious implementation of the system disclosed by Rakoshitz.

Rakoshitz discloses that certain applications are bandwidth-sensitive: *Rakoshitz, col. 4, lines 58-62* (see full quote above). Rakoshitz also discloses the traffic management cycle continuously creates/applies policies as well as reports/alarms: *Rakoshitz, col. 10, lines 3-7* (see

full quote above).

Given these teachings, a person of ordinary skill in the art would have readily recognized the desirability and advantages of implementing the system of Rakoshitz so as to incrementally restrict bandwidth allocated to the network traffic specifically exchanged with the proscribed application until an evasive action is detected, in order to determine a minimum bandwidth requirement, as discussed in Rakoshitz.

In referring to claim 15, in the implementation of the system of Rakoshitz discussed above, it would be obvious to record the minimum bandwidth level determined by decreasing the bandwidth, so as to provide the bandwidth required by the rogue application.

In referring to claim 16, in the implementation of the system of Rakoshitz discussed above it would be obvious to increase the bandwidth to the minimum level determined by decreasing the bandwidth below the threshold, so as to provide the bandwidth required by the rogue application.

In referring to claim 21, although Rakoshitz shows substantial features of the claimed invention, including the system of claim 20 (see 102 rejection above), Rakoshitz does not show the flow monitor decreasing the bandwidth allocated to the monitored network connection for each new flow of network traffic until an evasive action by the rogue application is detected. Nonetheless this feature is well known in the art and would have been an obvious implementation of the system disclosed by Rakoshitz.

Rakoshitz discloses that certain applications are bandwidth-sensitive: *Rakoshitz, col. 4, lines 58-62* (see full quote above). Rakoshitz also discloses the traffic management cycle continuously creates/applies policies as well as reports/alarms: *Rakoshitz, col. 10, lines 3-7* (see full quote above).

Given these teachings, a person of ordinary skill in the art would have readily recognized the desirability and advantages of implementing the system of Rakoshitz so as to decrease the bandwidth allocated to the monitored network connection for each new flow of network traffic

until an evasive action by the rogue application is detected, in order to determine a minimum bandwidth requirement, as discussed in Rakoshitz.

In referring to claim 22, in the implementation of the system of Rakoshitz discussed above (103 rejection of claim 21) it would be obvious to increase the bandwidth to the minimum level determined by decreasing the bandwidth below the threshold, so as to provide the bandwidth required by the rogue application.

In referring to claim 24, in the implementation of the system of Rakoshitz discussed above (103 rejection of claim 21) it would be necessary for the flow analyzer to identify an evasive action or other form of negative response taken by the rogue application, in order to determine a minimum bandwidth requirement, as discussed in Rakoshitz.

In referring to claim 27, in the implementation of the system of Rakoshitz discussed above (103 rejection of claims 21 and 22) it would be necessary for the steady state of bandwidth restriction to be sufficient to not trigger evasive action or other form of negative response by the rogue application in order to maintain the bandwidth required by the rogue application.

In referring to claim 30, although Rakoshitz shows substantial features of the claimed invention, including the system of claim 29 (see 102 rejection above), Rakoshitz does not show decreasing the bandwidth allocated to the monitored network connection for each new flow of network traffic until an evasive action by the rogue application is detected. Nonetheless this feature is well known in the art and would have been an obvious implementation of the system disclosed by Rakoshitz.

Rakoshitz discloses that certain applications are bandwidth-sensitive: *Rakoshitz, col. 4, lines 58-62* (see full quote above). Rakoshitz also discloses the traffic management cycle continuously creates/applies policies as well as reports/alarms: *Rakoshitz, col. 10, lines 3-7* (see

full quote above).

Given these teachings, a person of ordinary skill in the art would have readily recognized the desirability and advantages of implementing the system of Rakoshitz so as to decrease the bandwidth allocated to the monitored network connection for each new flow of network traffic until an evasive action by the rogue application is detected, in order to determine a minimum bandwidth requirement, as discussed in Rakoshitz.

In referring to claim 31, in the implementation of the system of Rakoshitz discussed above it would be obvious to increase the bandwidth to the minimum level determined by decreasing the bandwidth below the threshold, so as to provide the bandwidth required by the rogue application.

In referring to claim 33, in the implementation of the system of Rakoshitz discussed above (103 rejection of claim 30) it would be necessary for the flow analyzer to identify an evasive action or other form of negative response taken by the rogue application, in order to determine a minimum bandwidth requirement, as discussed in Rakoshitz.

In referring to claim 36, in the implementation of the system of Rakoshitz discussed above (103 rejection of claims 30 and 31) it would be necessary for the steady state of bandwidth restriction to be sufficient to not trigger evasive action or other form of negative response by the rogue application in order to maintain the bandwidth required by the rogue application.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Scott M. Klinger whose telephone number is (703) 305-8285. The examiner can normally be reached on M-F 7:00am - 3:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Glenn Burgess can be reached on (703) 305-4792. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Scott M. Klinger
Examiner
Art Unit 2153

smk

GLENTON B. BURGESS
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100